International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 17 (2015) pp 38391-38396

Secured Medical Image Transmission Through The Two Dimensional Chaotic System

I.Bremnavas
Dept. of Comp. Engg. and Networks
College of CS and IS
Jazan University, Jazan
Saudi Arabia
jmcnavas@gmail.com

I.Raja Mohamed
Dept. of Physics
B.S.Abdur Rahman Univesity
Chennai, Tamilnadu
India
irajamd@gmail.com

N.Shenbagavadivu
Dept. of Computer Applications
Anna University –BIT Campus
Trichy – 24, Tamilnadu
India
kshenthu@gmail.com

Abstract: In past few decades, many researchers have been intent more on using the field of chaos and its applications for their research. Particularly, medical image security using chaotic map. Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats were used, but digital images are the most popular because of their usage on the internet. This paper addresses the patient medical detail and medical image, text and pictorial form are encrypted and decrypted using two different set of algorithms. Advantage of this method is its security, which is provided by the chaotic signal. The chaotic signal generation and result analysis are done by Matlab 7.10.

Keyword: encryption, decryption; chaotic Henon map; cryptography; information hiding; image registration;

Introduction:

Internet is one of the most important factors of information processing technology. Cryptography as a technique for secured the secrecy of communication. It has been developed for many different methods to encrypts and decrypts data in order to keep the message secrecy. But it is sometimes not enough to keep the contents of a message secret, it may also be necessary to preserve of the message secret. The technique used to implement this is called Steganography, which is the process of hiding a secret message. The purpose of steganography is to maintain secret communication between two parties. The goal of Steganography is to mask the presence of communication making the message not discernible to the observer.

At present, medical images are being sent over computer networks. In this paper show how chaotic algorithms were used for a secured transmission of medical images. In order to do this, the patient medical data and images can be encryption and decryption in the Least Significant Bit (LSB) and Chaotic Henon map, the same images from different angle or two different images to be registered in order to apply this functionality at the application level. In this way, the functionalities of encryption and decryption of the patient medical data and images are inserted. Therefore this method guarantees for the protection of a medical image during transmission.

For example, when a doctor receives a patient detail after the patient visit, he often needs the expert opinion before giving the correct treatment for patient. One possible solution is to send patient medical images, along with the report over insecure communication network. Through insecure communication network is more complex. Here comes real security problem is raised when sending the medical data. When such a risk is present cannot be sent patient medical data and images and need to be given the better protection. Encryption and Decryption is the best form of protection in such cases.

Developments for the treatment using different techniques, communication of patient medical images and information go next to an increased risk for information in a digital format. Some possible factors for distant access increase the chances of losses [1]. Though, occurrence of these risks which given the need for the protection of patient medical information.

Many security algorithms are based on different chaotic map. Chaotic signal is used to hide the medical image in a unpredictable manner [2,3,4]. LSB method is used to hide patient data secretly. In this paper, we proposed a new medical image encryption and decryption. First, the patient medical data is embedded on patient medical image by LSB algorithm. Second, the encrypted patient medical images are registered and embedded by Choatic Henon map. Both the encrypted signals are embedded in the cover image.

Deterministic work of LSB and Chaos Implementation:

One of the techniques used in, steganography is to hide data behind images is called the least significant bit. Where in the LSB of each byte of the pixel of the text raster data is replaced with the single bit of the data to be hidden, i.e. the

eighth bit inside an image is changed to a bit of the secret message.

In spread spectrum techniques, hidden data is spread throughout the cover-image making it harder to detect [5]. A system proposed by Marvel et al. [1999] combines spread spectrum communication, error control coding and image processing to hide information in images [6]. Spread spectrum communication can be defined as the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies [6]. The Henon map is a prototypical two dimensional invertible iterated map represented by the state equations with a chaotic attractor and is a simplified model of the Poincare map for the Lorenz equation proposed by Henon in 1976 [7].

The two-dimensional Henon map is defined as follows:

$$X_{n+1} = 1 + Y_n - aX_n^2 \quad (1)$$

$$Y_{n+1} = bX_n \quad (2)$$

where *'a'* and *'b'* are constants. With initial point (x_0, y_0) the pair (x, y) is the two dimensional state of the system**.** When a = 1.4 and b = 0.3, the system is in chaotic state. [8,9,10,11].

Effectiveness of Schematics Diagram and algorithms of the proposed work:

In this paper, we try to find a simple, fast and secure algorithm for medical image encryption and decryption using the characteristics of chaotic functions by using larger key's space in the chaotic regions. The real robustness in chaotic based medical image encryption and decryption lies in choosing the better chaotic attractor. The Henon map is a two dimensional map in nature and also it is a pseudo random generator. The main advantage of this work is encryption and decryption made the system.

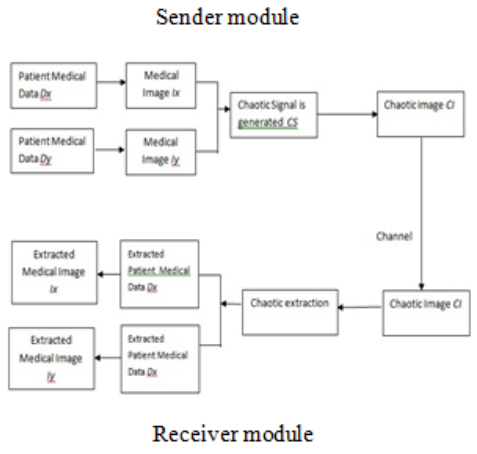

Fig 1: Encryption block, Insecure Communication link, Decryption block

Here Chaotic system generates more pixels using the Henon map equation. The image signals are bind up the pixels. Chaotic system is assigned the secret key for the image signals. Encrypted images are sent to insecure communication channel.

The schematic diagram of the chaotic encryption scheme is shown in Fig.1. The system consists of a sender module and a receiver module. The sender module consists of a LSB and chaotic Henon map. First, the patient medical data is encrypted on the patient medical image using LSB then an equivalent digital key sequence is generated from chaotic signals by a suitable threshold mechanism. The patients' medical data are encrypted using steganography least significant bits and pseudo random generator algorithm. The medical data of the patient is formatted in the following manner. Here, each organ of the human body is given an identical number so as to make the encryption procedure easier.

Age	Sex	Patient id	Organ details for example	description

For example, the patient date is formulate using the above format.

Age-42 , Sex-F , Patient id-237 , Organ number- 11 , Asymmetric growth. So the patient detail is 42F23711.

Then the patient medical image value is formed in one-dimensional array format. Based on the Chaotic Henon equations, signal is generated by both the x and y axis. The advantage of using the Henon map is send to two patient medical data embedded with respective patient images at a single transmission. For example, if it is needed to send two patient medical data and patient medical image in one transmission, the first patient data and patient medical image is added in x axis and then another one is added in y axis. Both the patient medical images are arranged in one dimensional array format. The Henon pixel data and patient medical image pixel data are embedded and the process is started in the key value a = 1.4 and b=0.3. So, both the data are stored in any location in the cover region.

The process of hiding information inside the image is achieved by LSB. The information that is to be stored inside the image is converted to Universal Text Format (UTF) i.e., 8,16,32 format based on the users need. The patient medical data is taken in the form of Age|sex|patient id|organ for example|description from the medical database. For example, the sample patient medical data is stored in the form Age-42, Sex-F , Patient id-237, Organ number- 11, Asymmetric growth. So the patient detail is 42F23711. The patient medical data is converted into binary format that contains sequence of 0's and 1's. The Pseudo random equation is applied to get the pseudo random sequence number. Each and every binary bit has a pseudo random number. The main work of this process is that the patient

medical data is embedded in the relevant patient medical image. The patient medical image data is already converted and stored in one-dimensional array using LSB. The patient medical image is converted in the form of UTF 8. The patient medical data is arranged in binary bits with the corresponding pseudo random number.

The converted value is being formed as array. The image in which information is to be stored is converted to pixel format, further converted to array format. The array format is divided into 8,16,32 blocks based on the information format. UTF format data is raster with the image using the random number generator. The random number generator finds the location in the image array where the data is to be raster.

The initial secret key value is selected in random manner. The user can fix dynamically the initial secret key. The encrypted two patient medical image and medical data are transferred through some secured channel in single transmission.

A. Proposed Algorithms:

In this section, we propose our algorithm gives better results on comparing with the other security algorithm.

Input : Medical image I_X and I_Y, and Medical data, D_X and D_Y.
Output: Encrypted Signal, ES

Step 1: Load a patient medical data, D_X and D_Y and its related patient medical image, I_X and I_Y from the database.

Step 2: Convert the patient medical image into one-dimensional array format named I_X then it is transformed in terms of UTF 8 bit binary format, U. Also convert the Patient medical data D_X, in binary form, B.

Step 3 : A pseudo random number is generated for all binary numbers.

Step 4 : The Binary data, B is embedded within U, using respective pseudo random number. This process creates an encrypted image, E.

Step 5: Generate the Chaotic Signal S using Henon equation

$$X_{n+1} = 1 + y_n - \alpha x_n^2 \quad \text{----} \quad (1)$$
$$Y_{n+1} = \beta x_n \quad \text{----} \quad (2)$$

Step 6: The patient medical data, D_X and patient medical Image I_X is embedded within the Chaotic Signal S using the following steps

6.1. Fixed the covered boundary region based on the size of an Image I_X.
6.2. The signal is assumed to be generated from the starting position of the boundary region
6.3. Set a key value K dynamically within the boundary region to represent the initial position.
6.4. The image value I_X is embedded with Chaotic signal S from K.

Step 7: The above step 6 is repeated for the patient medical data D_Y and Medical Image I_Y and with the same key value, K.
Step 8: The encrypted signal (ES) is transferred along with the key value K(The key value is embedded in a standardized position of the signal ES).

B. The Proposed Extraction algorithm

Input : Encrypted Signal, ES
Output: Patient Medical data, D_X and D_Y, Patient Medical Image, I_X and I_Y.

Step 1: Received the encrypted signal, ES from the open communication channel.

Step 2: Retrieve the key value K from encrypted signal ES.

Step 3: Generate the Chaotic signal S using Henon equation

$$X_{n+1} = 1 + y_n - \alpha x_n^2 \quad \text{----} \quad (1)$$
$$Y_{n+1} = \beta x_n \quad \text{----} \quad (2)$$

Step 4 : Subtract the received encrypted signal, ES with the raw Henon signal, S using the key value K, to obtain a one-dimensional array for each medical image Ix and Iy.

Step 5 : Construct the resultant image from the one-dimensional array.

Step 6 : Divide the encrypted medical image, E into 8 bit blocks respective of the data size.

Step 7 : Extract the patient medical data, D_X and D_Y from the binary 8 bit blocks using the generated sequence of pseudo random numbers.

Step 8 : Convert the binary data, B into UTF value, U.

Step 9 : Convert the UTF value, U into text format.

Step 10 : Extract the resultant images I_X and I_Y from the one-dimensional array.

Result Analysis:

The proposed encryption and decryption algorithm is implemented in MATLAB for computer simulations. The two test patient medical data and their corresponding patient medical images (1) and (2) are registered then encrypted and decrypted using chaotic system using the two dimensional Henon map equations.

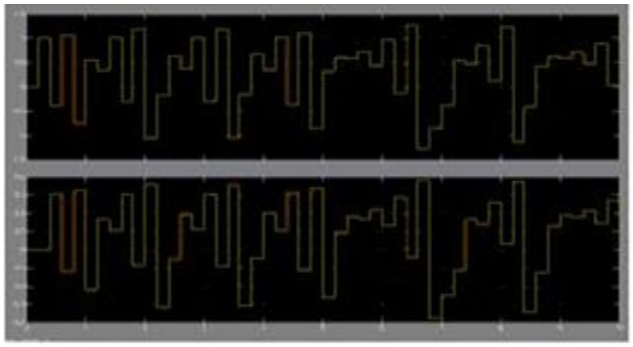

Fig 2 illustrates Time series of system variables x and y

Encryption and decryption time will be in ml sec. (200 kSa / s)

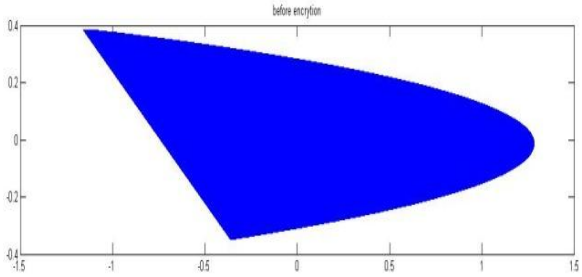

Fig 3 depicts the phase filled Henon map in which the chaotic regions is shown sequence with -1.5 to 1.5 with 0.4 as the initial condition

This technique used here is to assess the quality of registration of pairs of photographs of human heart and human eye viewed from two different patients medical details. To register such two patient medical data and their corresponding medical image signals are encrypted to LSB then it is encrypted by chaotic system. Patient medical data and medical images are registered and then send it to insecure communication channel.

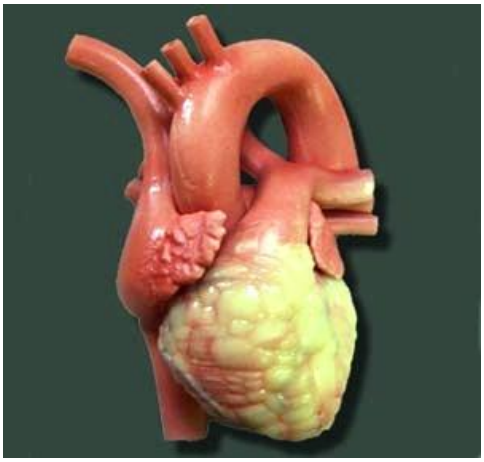

Fig 4.Image (1) before Encryption

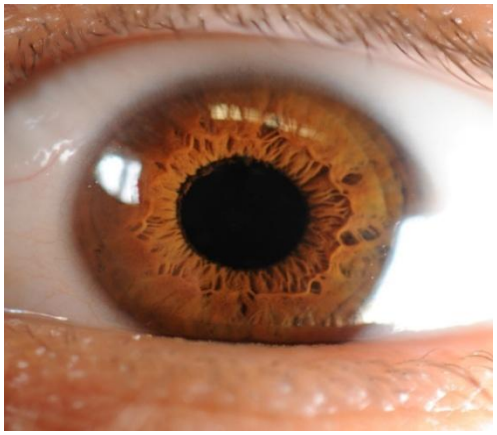

Fig 5. Image (2) before Encryption

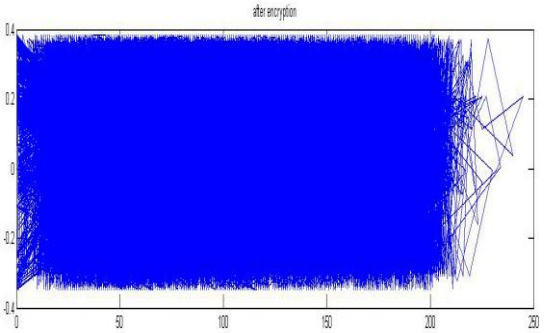

Fig 6. Signal after encryption.

Both image 1 and image 2 are encrypted by the carrier chaotic signal with two different parameters.

Fig 6 shows the encrypted chaotic sequence with two patient medical data and medical registered images. The generated chaotic Henon equation in the form of signal and both two patient data and images are encrypted in the pixel format to add the above chaotic signal in the covered part.

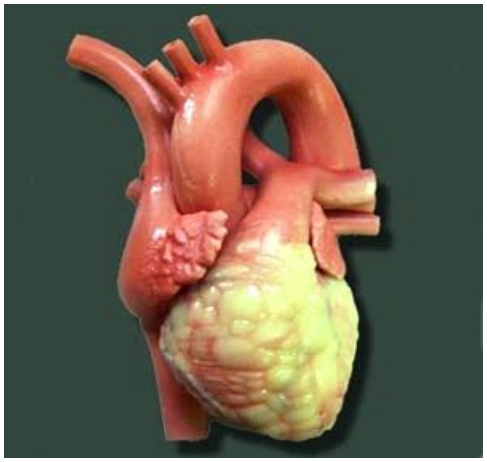

Fig. 7 Image (1) after Decryption

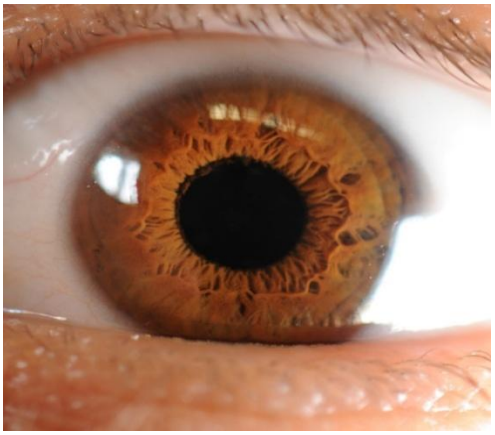

Fig.8 Image (2) after Decryptions

The two patient test data and images image 1 and image 2 each of size of 256 x 256 (kb) are registered, encrypted and decrypted using chaotic system using the two dimensional Henon Map equations.

Performance Measurement:

Two of the error metrics are used to compare the various image compression techniques are the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) to achieve desirable compression ratios. The MSE is the cumulative squared error between the compressed and the original image, whereas PSNR is a measure of the peak error. The mathematical formulae are

$$PSNR = 20 \log \left[255 / \sqrt{MSE} \right]$$

------ 1

$$MSE = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - I'(x,y)]^2$$

------- 2

where I(x,y) is the original image, I'(x,y) is the approximated version and M,N are the dimensions of the images. A lower value for MSE means lesser error, and as seen from the inverse relation between the MSE and PSNR, this translates to a high value of PSNR. Logically, a higher value of PSNR is good because it means that the ratio of signal to noise is higher. Here, the signal is the original image, and the noise is the error in reconstruction. So, if you find a compression scheme having a lower MSE (and a high PSNR).

Medical Image	Size of the Image	Proposed Choatic Henon map	
		PSNR (dB)	MSE
Image (1)	411 x 291	53.6437	0.2810
Image (2)	595 x 420	60.1956	0.0530

Medical Image	Size of the Image	PSNR (dB)	
		Chaotic Henon Map	Watermarking
Image (1)	411 x 291	53.6437	55.142
Image (2)	595 x 420	60.1956	62.146

From the above table, it is clear that the proposed system results in a maximum Peak Signal Noise Ratio value compared to Watermarking, which produces a better quality image.

Conclusion:

In this paper we proposed a new encryption and decryption method addressed the patient medical details in text form and medical image of the organ in pictorial form which have been encrypted and decrypted using two different set of algorithms. The main advantage of this method is the security, which is provided by the chaotic signal. The chaotic signal generation and the result analysis are done by using the Matlab 7.10. The PSNR and MSE value is calculated and plot is also shown.

References:

[1] Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs "Implementation of LSB Steganography and Its Evaluation for Various Bits" Digital Information Management, 2006 1st International conference.pp 173-178,2007.

[2] Z.H. Guan, F. Huang, and W. Guan, "Chaos- Based Image Encryption Algorithm," *Physics Letters A*, vol. 346, 2005, pp. 153– 157.

[3] M. Suneel, "Cryptographic Pseudo-random Sequences from the Chaotic Henon Map," *Sadhana*, vol. 34, no. 5, 2009, pp. 689–701.

[4] V. Patidar, N.K. Pareek, G. Purohit, and K.K. Sud, "Modified Substitution–Diffusion Image Cipher Using Chaotic Standard and Logistic Maps," *Commun Nonlinear SciNumer Simulat*,vol. 15, 2010, pp. 2755–2765.

[5] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*, 47:10, October 2004

[6] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", *IEEE Transactions on image processing, 8:08*, 1999

[7]Henon M, *A Two-Dimensional Mapping with a Strange Attractor*, *Communication in Mathematical physics*, vol. 50, 1976, pp. 69–77.

[8]Forre R, "The Henon Attractor as Key Stream Generator," *Abstracts of Eurocrypt 91*, 1991, pp. 76–80.

[9] Alghamd A.S, Ullah H, Mahmud M, and Khan M.K., *Bio-Chaotic Stream Cipher- Based Iris Image Encryption*, Proceedings of the International Conference on Computational Science and Engineering, 2009, pp. 739–744.

[10] Yu X.Y., Zhang J., Ren H.E., Xu1 G.S., and Luo X.Y., *Chaotic Image Scrambling Algorithm Base.*

[11] I. Bremnavas et al., *Elixir Comp. Sci. Engg. 54 (2013) 12598-12602*

Dr. I.BREMNAVAS obtained his B.Sc Degree in Mathematics. He received M.Sc., degree in Information Technology and M.Phil degree in Computer Science from Bharathidasan University, Trichy, Tamil Nadu, India in 2002 and 2004 respectively. Also obtained M.C.A., degree and MBA., degree from Periyar Unviersity, Salem and Indira Gandhi National Open University (IGNOU) from New Delhi in 2007 and 2010. He has nearly fifteen years of teaching experience. Currently, he is working as a Assistant Professor in Computer Networks Department, Jazan University, Jazan, Saudi Arabia. He has over ten National and International research publications, presented thirteen Conference Papers and published one book entitled "Computer and Communication Network".

Dr. I.RAJAMOHAMED, Professor and Head in Physics Department, B.S.Abdur Rahman University, Chennai, Tamil Nadu, India. He obtained his B.Sc Degree in Physics. He received M.Sc., & M.Phill degree in Physics in 1987 and 2000 respectively. Also obtained Ph.D., degree in 2007. He has nearly two decades of teaching experience. He has over ten National and International research publications, presented more than ten Conference Papers.